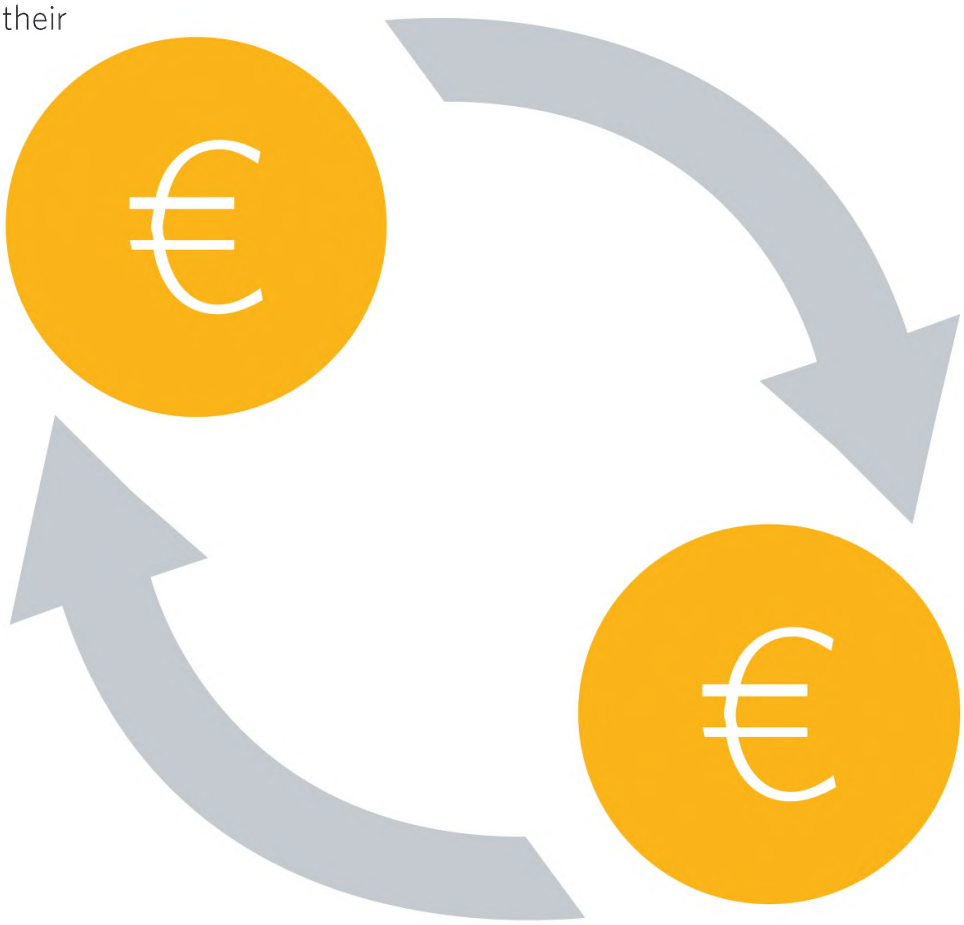
Cashback best practices

Cashback publishers are an essential component of the majority of affiliate marketing programmes and their continued success is important to the wider industry. To preserve advertiser confidence in the model, Awin has produced the following guidelines and encourage all cashback and loyalty publishers to adhere. Whilst compliance will not be punitively enforced, insight into current practices must be provided.

Awin believe that by offering advertisers assurances that cashback sites monitor their member's behaviour, alongside transparency into a publisher's current practices, advertisers will be able to make informed decisions on whom to partner with, maintaining confidence in the sector.



Overview

Cashback Publisher Best Practice Guidance

Enforcement of Guidance	Commission threshold and enforcement
Click Ref Data	Unique Customer ID Transaction data – time; click-to-sale; product info Toolbar implementation
Member Checks	Confirmed banking betails Repeat transactions Blocking users
Advertiser Requests	Payment methods Transaction restrictions
Fraud Prevention Measures	Awin publisher account overview Suggested measures to implement

1. Enforcement of Guidance

Publishers of all sizes are encouraged to comply. Any publisher found to be non-compliant must submit the timescales it will take to become compliant and these will be shared with advertisers they promote. Failure to do so will also be shared.

2. Click Ref Data

i. Unique Customer ID:

Cashback publishers must allocate each user a unique ID and make this available to Awin via the click ref parameter.

Cashback publishers must make every effort to establish any duplicate or linked user accounts. This may be via confirmed banking details, physical address data, or other unique identifiers provided at the point of user sign-up.

Where a user with multiple accounts is discovered, they must be informed that such activity is not permissible, and a single account is required.

ii. Transaction Data:

Cashback publishers must maintain records of member transaction data and make this available to Awin upon request.

Transaction data must include the click-to-sale time; time and date of the completed transaction; the advertiser and product information; user IP and location, as far as is available. The total of the number of transactions attempted/completed must also be made available on a per-user basis to assist and support Awin compliance standards.

Where duplicate IP information is discovered across multiple user accounts, this must also be flagged to Awin for further investigation.

A monthly summary of suspected user fraud and illegitimate or suspicious transaction data must be provided to Awin monthly, or upon request.

iii. Toolbar Recognition

Should a cashback site choose to offer a toolbar or browser extension to their customers, this activity must be easy to separate from standard cashback activity by passing a unique identifier in a click reference field, or tracked via a separate publisher account.

3. Member Checks

i. Confirmed Banking Details:

To mitigate the risk of fraud, and to ensure an appropriate level of due diligence, it is recommended that cashback publishers seek to confirm that banking details match user information provided at the point of sign-up. This includes, but is not limited to, names, addresses/country of residence, and date of birth, where possible.

ii. Repeat Transactions:

Cashback publishers must actively monitor and flag repeat purchases, especially if they generate a high commission (£20+), or if there are repeat attempts to purchase identical products through the same advertiser over the course of every 30-day period, as a minimum.

Any such examples must be flagged to Awin for further review to establish their legitimacy.

As above, any duplicate IP information must also be flagged for further investigation.

A specific focus in this area must be given to subscription or contract-based, long-term products, especially within the finance and telecoms sectors, but with appropriate timescales applied, such as within a 12-month period.

iii. Blocking Users:

Where a cashback publisher is unable to verify member identity, and/or if persistent abuses of the cashback facility or multiple illegitimate transactions are discovered, individual members must be blocked or removed from the site, or from accessing specified advertisers, as appropriate.

Any newly-created user accounts must be reviewed against previously blocked user data to prevent the same issues occurring, as far as is practicable.

4. Advertiser Requests and Instruction

i. Payment Methods:

Cashback Publishers must comply with any request from an Advertiser to pay commission/cashback in a specified form; this may include, but is not limited to:

BACS payment	Stored-value cards	Verified PayPal accounts	Vouchers	Charitable Donations

ii. Transaction Restrictions:

Cashback publishers must implement any transaction restriction(s) defined by an advertiser, such any limit on the number of transactions per member, per product, within a defined period

5. Fraud Prevention Measures

i. Awin publisher account overview:

Cashback publishers must maintain an accurate Awin publisher account overview which details their fraud prevention measures.

Where this is maintained as a summary, a full breakdown must be available upon request to Awin and any Advertiser

ii. Suggested measures to implement:

Effective member due diligence	Confirm banking details	Confirm member address where possible, and location as a minimum	Transaction data monitoring, including IP	Monitoring and checks to identify users with multiple accounts